Sniffing Basics – MAC Address

iSECUR1TY
INTEGRATED SECURITY SOLUTIONS
مركز الدورات التدريبية

- Each network card has a physical static address assigned by the card manufacturer called MAC address (Media Access Control).
- This address is used between devices to identify each other and to transfer packets to the right place.
- Each packet has a source MAC and a destination MAC.

Sniffing Basics – MAC Address

iSECUR1TY
INTEGRATED SECURITY SOLUTIONS
مركز الدورات التدريبية

We can change our MAC address value that is stored in the memory using a program called macchanger like so:

```
> ifconfig [INTERFACE] down
> macchanger -m [MAC] [INTERFACE]
> ifconfig [INTERFACE] up
```

[interface] = your wifi card name.

[MAC] = the mac address you want to use.

Packet Sniffing Basics
MAC Address

iSECUR1TY
INTEGRATED SECURITY SOLUTIONS
مركز الدورات التدريبية

Question: if the MAC address is used to ensure that each packet gets delivered to the right place then how can we capture it.

Answer: Yes and no , it is used to sent packets to the right destination , and we as hackers can only receive packets that are sent to our MAC address , but this only applies to the default mode of your wireless card , which is managed mode , however there is mode that allows us to capture all the packets in our wi-fi range , not only the ones sent to our device , hence the name monitor mode.

Packet Sniffing Basics
Airodump-ng

iSECUR1TY
INTEGRATED SECURITY SOLUTIONS
مركز الدورات التدريبية

Airodump-ng is a program part of aircrack-ng package , its a packet sniffer that allows us to capture all the packets that are in our wifi card range. We can also use it to just scan all wifi networks around us and gather info about them.

Using Airodump-ng:

1. Enable monitor mode:

```
> airmon-ng start [interface]
```

2. Start airodump-ng

```
> airodump-ng [interface]
```

Targeted packet sniffing

iSECUR1TY
INTEGRATED SECURITY SOLUTIONS
مركز الدورات التدريبية

We can launch airodump-ng on a specific target

```
> airodump-ng --channel [channel] --bssid [bssid] --write [file-name] [interface]
Ex: airodump-ng –channel 6 –bssid 11:22:33:44:55:66 –write out mon0
```

Now all the data will be stored in the file name specified after the –write option. We can analyse this data using wireshark (we shall explain how to use wireshark later in the course). The only problem is that the collected data will not be much of use if the target network uses encryption.

Deauthentication Attacks Theory

iSECUR1TY
INTEGRATED SECURITY SOLUTIONS
مركز الدورات التدريبية

This attack is used to disconnect any device from any network within our range even if the network is protected with a key.

- Hacker sends deauthentication packets to the router pretending to be the target maching (by spoofing its MAC address).
- At the same time , the hacker sends packets to the target machine (pretending to be the router) telling it that it needs to re-authenticate itself.

Deauthentication Attacks Practical

To de-authenticate all clients in a specific network

```
> aireplay-ng --deauth [number of packets] -a [AP] [INTERFACE]
Ex: aireplay-ng --deauth 1000 -a 11:22:33:44:55:66 mon0
```

To de-authenticate a specific client in a network

```
> aireplay-ng --deauth [number of deauth packets] -a [AP] -c [target] [interface]
Ex: aireplay-ng --deauth 1000 -a 11:22:33:44:55:66 -c 00:AA:11:22:33:44 mon0
```

Deauthentication Attacks
airdrop-ng

iSECUR1TY
INTEGRATED SECURITY SOLUTIONS
مركز الدورات التدريبية

Airdrop-ng is a script that is carries out the previous attack automatically based on specific rules. Targets are specified based on their MAC address or hardware manufacturer (eg: apple , broadcom ..).

use:

```
> airodump-ng --write [filename] --output-format csv [interface]
> airdrop-ng -t [csv-file] -r [rules-file] -i [interface]
Ex: airodump-ng --write out --output-format csv mon0
Ex: airdrop-ng -t out-01.csv -r rules -i mon0
```

Note: refer to the attached “rules.txt” file for examples of rules.

Creating a fake access point (honeypot)

iSECUR1TY
INTEGRATED SECURITY SOLUTIONS
مركز الدورات التدريبية

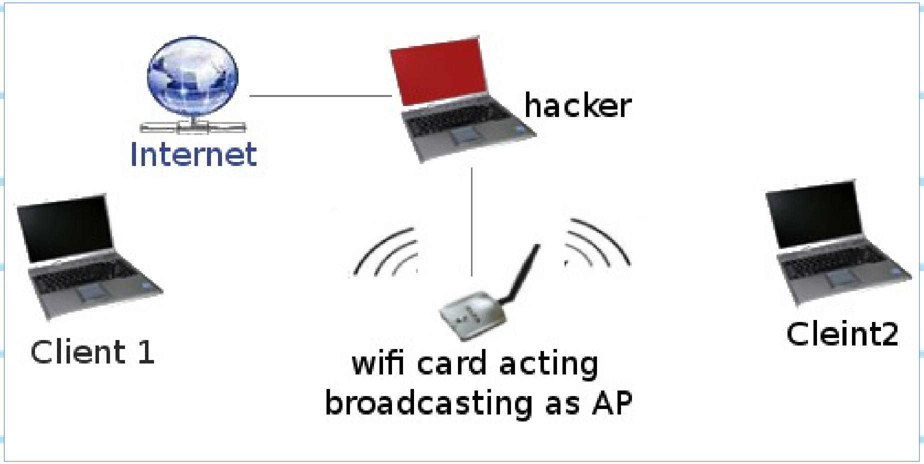
Fake access points can be handy in many scenarios , one example is creating an open AP , this will attract a lot of clients , many of which will automatically connect to it. Then we can sniff all the traffic created by the clients that connect to it , and since its open , the traffic will not be encrypted !

Creating a fake access point (honeypot)

iSECUR1TY
INTEGRATED SECURITY SOLUTIONS
مركز الدورات التدريبية

In order to do this , we need two cards:

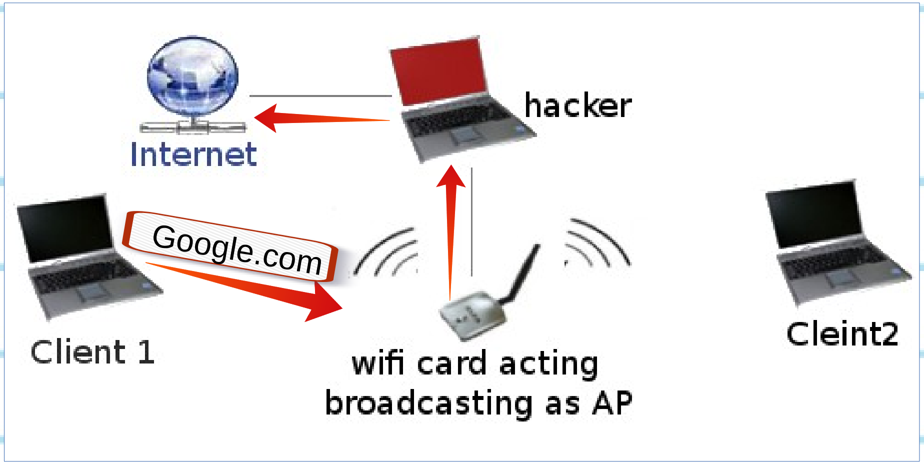
1. One connected to the internet.
2. Wifi card to broadcast as an access point



Creating a fake access point (honeypot)

iSECUR1TY
INTEGRATED SECURITY SOLUTIONS
مركز الدورات التدريبية

Clients now send requests to the hackers wifi card , the hacker sets up his machine so that every request coming from the wifi card is forwarded to the 2nd card thats connected to the internet.



Creating a fake access point (honeypot)

The response comes back from the 2nd card , through the hackers machine to the wifi card which forwards it to the client that requested it.

